

EXHIBIT E

1.	On behalf of	Claimants
2.	Initials/Surname of witness	C J R Goodfellow
3.	Statement No	1
4.	Date	14 September 2018

Claim No. HC-2015-001324

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
BUSINESS LIST (ChD)

B E T W E E N:

(1) ACL NETHERLANDS B.V. (AS SUCCESSOR TO AUTONOMY CORPORATION LIMITED)
(2) HEWLETT-PACKARD VISION BV
(3) AUTONOMY SYSTEMS LIMITED
(4) HEWLETT-PACKARD NEW JERSEY, INC

Claimants

-and-

(1) MICHAEL RICHARD LYNCH
(2) SUSHOVAN TAREQUE HUSSAIN

Defendants

WITNESS STATEMENT OF CHRISTOPHER JAMES ROBIN GOODFELLOW

I, CHRISTOPHER JAMES ROBIN GOODFELLOW of The Old Manse, 49 High Street, Burwell, Cambridge, Cambridgeshire, CB25 0HD STATE AS FOLLOWS:

1. I make this Witness Statement on behalf of the Claimants in connection with the above named proceedings. Except where it otherwise appears, the facts and matters to which I refer in this Witness Statement are within my own knowledge and are true. Where facts are from another source, I identify the source and I believe them to be true. Where the source of my understanding or information is the Claimants' solicitors, I have identified this in this Witness Statement but without any waiver of legal professional privilege.
2. I have not attached the documents to which I refer in this Witness Statement. Instead I have provided document references for those documents. I understand that the document references are the Document Production IDs allocated to the documents by the parties as part of the disclosure process in the current proceedings. I have relied upon these documents to refresh my recollections and refer to the specific content of a number of them.

Professional history and background

3. I joined Autonomy Corporation plc ("**Autonomy**") in October 2004 as a sales engineer, before becoming the EMEA (Europe Middle East & Africa) pre-sales manager. I subsequently transitioned into the role of Director of Global Accounts and I held that position until 2008. Between 2009 and 2013, I was Chief Technology Officer of Infrastructure at Autonomy, following which I became the Chief Technology Officer of HP HAVEn OnDemand (Hewlett Packard having acquired Autonomy by that point). I moved over to Micro Focus when it acquired the software business from Hewlett Packard Enterprise but I recently left on 28 February 2018.
4. After Autonomy's acquisition of ZANTAZ Inc. ("**Zantaz**") in July 2007, I had oversight of Autonomy's hosted offerings, in particular Digital Safe (Autonomy's principal digital archiving solution). Between 2008 and 2011 (which I understand from the Claimants' solicitors to be the relevant period for the purpose of these proceedings), in my roles as Director of Global Accounts and Chief Technology Officer of Infrastructure, I worked with a number of teams within Autonomy, including the Digital Safe Sales team, Roger Wang's Digital Safe Product Development team, Robert Desroches' Digital Safe Operations team and the post-Sales support team for Digital Safe customers.
5. Between 2008 and 2011, I reported directly to Dr Peter Menell, Chief Technology Officer at Autonomy. I was also in frequent contact with Sushovan Hussain (Autonomy's Chief Financial Officer). I spoke to him on a weekly basis and sometimes daily depending on what was happening at any particular time. I had occasional involvement with Dr Michael Lynch (Autonomy's Chief Executive Officer).

Digital Safe

6. Digital Safe is fundamentally a compliant data archive. If a customer is regulated, which is often the case in the financial services industry, then that customer will be under an obligation to maintain a record of its communications (primarily emails) pursuant to SEC Rule 17a-4. Most of Autonomy's largest Digital Safe customers were banks seeking to comply with the regulations. It was generally understood that, to achieve compliant data archiving, a third party needed to have access to the customer's data without having to go through the customer. This requirement was satisfied if the customer's data was hosted in Autonomy's data centres or if the data was held on the customer's premises but Autonomy had constant remote access to it. When customers purchased Digital Safe they were in effect buying a third party in Autonomy; this was a key part of the service. Between 2008 and 2011, Autonomy did not have any meaningful competition; Digital Safe was the industry-leading compliant archiving solution and it was the most scalable

offering on the market. It was an extremely successful product, especially in light of Zantaz's growing customer-base following the financial crisis in 2008.

7. The Digital Safe solution was Autonomy's hosted archiving offering, although on occasion a customer asked for it to be set up on their own premises. In the case of a hosted Digital Safe customer, the entire Digital Safe system (comprising the hardware, the software and the network connecting it all together) sat in Autonomy's data centres. Autonomy was responsible for everything including managing the data centre, maintaining the Digital Safe hardware and software and providing the people who managed and serviced Digital Safe.
8. The Digital Safe software performed a "capture and index" function. Customers sent data to Digital Safe and Autonomy would "capture" it by processing and storing the data in accordance with the regulations (for example, ensuring the data is stored in two locations and in such a way that it cannot be tampered with). Autonomy then "indexed" the data so that it could subsequently be searched and emails could be retrieved (e.g. so that discovery could be performed in the litigation context).
9. The capture and index process occurred largely automatically by virtue of the Digital Safe software. However, Autonomy's Operations team needed to do a lot of work to keep the "automatic" capture and index process running. Autonomy monitored the entire Digital Safe system (including the software) on a 24/7 basis. Autonomy looked after and fixed the hardware when it broke, supported the network (which connected the different parts of the Digital Safe solution together) and monitored the software for issues. There was a dedicated software monitoring team whose job it was to sit and watch computer screens for a sign of problems. There was another team that responded when software issues arose and there was a third software team that drew patterns between recurring issues. Although the capture and index process was automatic, a significant degree of human involvement was required to sustain it. Autonomy regularly dealt with software issues that required corrective action, such as security issues and corrupt indexes. Customers did not have the expertise or the necessary access to Autonomy's data centres to deal with such issues themselves. I would estimate that when I left Micro Focus in February 2018, there were approximately 300 people providing Digital Safe services as their full-time job. Between 2008 and 2011, there were fewer people than this, but there were still a significant number.
10. When Autonomy started selling licences to Digital Safe in around 2008 (as explained further at paragraph 13 below), it generally charged an annual maintenance and support fee set at 5% of the licence fee. This fee only accounted for a limited set of services relating to the software licence: telephone hotline support, bug fixes and upgrades. I will call these services "support services" below in order to differentiate them from the

services that I have described at paragraph 9, which I will call "managed services". The managed services above went way beyond the support services that customers were entitled to receive as part of the 5% maintenance and support. My understanding is that, both before and after the acquisition of Zantaz by Autonomy (and the move towards selling licences), the cost of the managed services was incorporated into the ongoing storage fee. I would estimate that for a big bank, 75% of the storage rate was attributable to the actual storage element and the remaining 25% was attributable to the cost of providing the managed services. My view is that the managed services represented at least 20% of the overall value of a hosting contract.

11. The engine within Digital Safe that indexed the data and enabled it to be searched and retrieved either relied on Lucene software or IDOL software. Historically, Zantaz customers all used Lucene as the indexing engine. After Autonomy's acquisition of Zantaz, there was a big push to create an IDOL safe that was powered by Autonomy's IDOL software instead of Lucene. Generally speaking, new customers who bought Digital Safe during the Autonomy era were sold IDOL safes whereas existing customers remained on Lucene safes. I do not recall any of Zantaz's pre-acquisition customers (including all of its banking and other biggest customers) completing the migration from Lucene to IDOL safes. In theory, an IDOL safe had additional capabilities over and above a Lucene safe. However, not all of IDOL's analytical functionality was enabled in customer safes as it would have made Digital Safe more expensive to run. Autonomy and its customers did not during the relevant period (2008 to 2011) achieve the full potential of an IDOL safe, and for this reason Lucene safes still exist; the most important Digital Safe customers still used them at the time I left Micro Focus earlier this year. A successful IDOL safe would certainly have been preferable to a Lucene safe. As it was, though, it was expensive and inefficient for existing customers to switch from Lucene to IDOL without having a clear path to achieving value. Dr Lynch suggests at paragraph 137.2 of his Amended Defence and Counterclaim (the "**LADCC**") that embedding IDOL into Digital Safe led to the product receiving "*new regulatory accreditation*". I cannot think of any way in which IDOL enabled Digital Safe to achieve new regulatory accreditation – the regulatory accreditations of IDOL and Lucene safes were identical as far as I am aware.
12. I understand from the Claimants' solicitors that Chris Yelland (Autonomy's CFO from 2012 onwards) refers in his Witness Statement to various discussions I had with him about, amongst other things, storage in Digital Safe arrangements as compared with e-Discovery (which allowed customers to review and code their data for the purpose of discovery in litigation). On a per MB basis, the cost of eDiscovery storage was higher than the cost of Digital Safe storage. This was due to the need, in the eDiscovery context, for reviewers to have instantaneous access to documents and because reviewers tagged documents (i.e. as relevant or not relevant). This tagging process created additional data

to be stored, so new data was constantly being generated throughout the review process. The cost of and infrastructure for storage in an eDiscovery context was consequently quite different to the Digital Safe context.

Selling licences to Digital Safe

The SaaS model versus the licence model

13. Around the summer of 2008, Autonomy began charging customers fees for a licence to use the Digital Safe software, along with separate storage and maintenance and support charges. My understanding is that Autonomy recognised the licence revenue upfront and the storage and maintenance and support revenue over time. Previously, under Zantaz's SaaS (Software as a Service) model, customers paid ongoing storage fees and Zantaz recognised the revenue it received over the term that it provided the services. Autonomy sold Digital Safe licences to both new customers and existing customers. For existing customers, Autonomy reduced the customers' existing ongoing storage rates in exchange for the upfront licence fee. For new customers, Autonomy highlighted the discount available under the licence model as compared with SaaS pay as you go pricing. The licence model meant more revenue for Autonomy in the short term, but less revenue under the new arrangement as a whole given that Autonomy reduced ongoing storage rates significantly in order to create overall savings for the customers (and incentivise them to purchase the licence).
14. It was clear to me at the time that Autonomy's management team was aggressive with its accounting policies. Although I was not part of the finance team, I worked in Autonomy's Cambridge office with various members of that team, including Mr Hussain and Steve Chamberlain, and they would often ask me questions to assist with their accounting analysis and try to justify their approach. My understanding was that the reason why Autonomy moved to the licence model was so that it could accelerate the recognition of revenue. The trade-off for the earlier recognition of revenue was a reduction in overall revenue to Autonomy from what was, in actual practice, the same business and service relationship. Customers who acquired a licence to the Digital Safe software received the same service as those who did not; nothing changed from a technical perspective. I viewed the move towards the new licence structure as being driven by accounting rather than business or technical issues.
15. Dr Lynch asserts that the SaaS model had "unsatisfactory customer retention qualities" (paragraph 143.1, LADCC) and "Had it sought to continue the old product and pricing structure, Autonomy could not have expected adequately to attract or retain customers" (paragraph 145.4, LADCC). I disagree with these statements. Generally speaking in 2008 to 2011, the market had moved away from licence models towards subscription models.

Customers generally preferred the SaaS model where they paid for their hosting services over time. In my experience it was Autonomy who was offering the licence model as opposed to customers requesting it. As to whether Autonomy could have adequately retained its customers under the SaaS model, in fact very few large customers left Autonomy and moved their data out of Digital Safe (under whatever pricing model). Customers often stored huge volumes of data in Digital Safe and there were risks associated with migrating that data to a new provider. Customers would need to ensure that the migration was compliant with the regulatory requirements and that there was a clearly auditable process in place to demonstrate that fact. There was a significant risk of regulatory action in the event of an imperfect process. This risk typically meant that large financial services customers had limited appetite for migration.

16. Dr Lynch states that Autonomy obtained longer term commitments from customers who moved from the SaaS to the licence model: "*Customers were more likely to remain in a longer term relationship*" (paragraph 138.5, LADCC). When customers left Autonomy (which did not happen often), it was generally for one of two reasons: either because they thought the cost of the service was too high or because they were dissatisfied with the service. Given that Autonomy offered customers overall cost savings in return for purchasing licences, I can see how the licence model might have meant that fewer customers considered leaving for cost reasons. Although the Digital Safe service provided under the SaaS and licence models were the same, if customers were dissatisfied with that service, I can see how they might have been less willing to give their business to another provider if they had made an upfront payment. In my view, these retention benefits were not dependent on customers purchasing licences – Autonomy could have achieved the same results with the SaaS model, by simply reducing the customer's overall spend and/or including an upfront pre-payment. And in any event, as I have said, there was no meaningful competition for Digital Safe at the time for larger regulated customers, the relationship with whom was usually long-lasting.
17. Dr Lynch refers to "*the valuable upsell... opportunities presented by the Hybrid Model*" (i.e. the licence model) (paragraph 145.4, LADCC). Autonomy was always interested in opportunities to upsell new repositories, modules, applications and functionality as technology developed. Good examples of this in the Digital Safe context were eDiscovery and Supervisor S6 (which enabled customers to monitor the communications of certain regulated individuals to ensure compliance with the customer's policies), which were sold to a number of Digital Safe customers. These products could, though, be upsold to customers on a SaaS basis, so to the extent there were any upsell opportunities, these were not limited to customers on the licence model. A more significant upsell opportunity arose as regards the volumes of data that a customer might store in a Digital Safe. I think it likely that the much reduced storage rates under the licence model

encouraged customers to put more data into Digital Safe than they might otherwise have done. This would have led to increased revenues, but, given the reduced storage rates, at lower margins. JPMC is an example of this. JPMC was converted to a licence arrangement. The storage rates agreed with JPMC were so low that it tried to put everything it could into its Digital Safe archive. This was, though, something of a double edged sword. Although it created more data volume, storage revenues on a per MB basis were so low after the restructure that they were not much more than Autonomy's associated costs. Furthermore, and once again, any increase in data volumes stemmed from the reduced hosting charges, so the same result could have been achieved with the SaaS model by including an upfront pre-payment and reducing the ongoing storage charges.

Customer use of a Digital Safe licence

18. Whether or not a customer who purchased a licence to the Digital Safe software could set up and make use of Digital Safe without Autonomy's managed services boils down to a debate between the technically possible and the practically possible. Technically speaking, if I and a group of ex-Autonomy employees that I carefully selected got together, we could make use of the Digital Safe software to set up Digital Safe without any input from Autonomy. However, practically speaking, if you dumped the Digital Safe software on someone with no knowledge of Digital Safe (and to be clear, there were no customer facing instruction manuals on how to implement, use or manage Digital Safe), that person could not set up and use Digital Safe. Only people who are extremely familiar with Digital Safe (i.e. people who work or have worked at Autonomy) can readily understand it. Implementing and operating Digital Safe requires a huge amount of technical knowledge. Hypothetically speaking, if you gave the Digital Safe software to me and I had no prior knowledge of Digital Safe, in time, given my technical abilities, I could probably work out what to do with it, but commercially it would be unviable because the process of figuring it out would cost too much and take far too long. I doubt very much that the technical teams within the financial institutions to whom Autonomy typically sold Digital Safe licences would be able to make any sense of the Digital Safe software. In reality, I cannot imagine any customer implementing it successfully, and I would certainly not invest in any business that attempted to do it. So although in theory the licence gave customers the right to operate Digital Safe themselves, in practice this right by itself was meaningless because customers were dependent on Autonomy's implementation and ongoing services. Value added resellers ("**VARs**") could not add value to a Digital Safe transaction, save from a marketing perspective, because they could not perform the necessary services. If VARs such as Capax Discovery LLC and MicroTech LLC were trained to implement Digital Safe on-premise, I would certainly expect to have known about it.

19. Digital Safe software, on its own and without the associated implementation and managed services which only Autonomy could provide, was of limited value to a customer. A customer might buy a licence to use Digital Safe software but, in practice, the customer would not then be able to do anything with it. The only party to whom it could turn to build a Digital Safe system (to source and configure the necessary hardware etc. and load the software onto it) was Autonomy. Once implemented, a Digital Safe archive could only be operated with Autonomy's managed services. Without those services, the system would experience multiple individual failures and would ultimately stop working altogether. I suppose the Digital Safe solution could have evolved to become a standalone piece of software that was possible for a customer to set up and use on its own premises without Autonomy's involvement. However, Autonomy never took steps to adapt Digital Safe in this way. We had other archiving solutions, e.g. EAS and CAMM, that were designed for customers to take on premise.
20. Dr Lynch says that *"Purchasing the licence upfront was attractive to customers because it offered control by the customer over its own data and therefore protected the customer in the event that it needed to move its data to a new producer or to an on-premise set up. Given that the customer had that control and protection, customers had less concern about signing up for longer term arrangements because they still had the flexibility to move away if they wanted to do so"* (response 6, Dr Lynch's Response to the Claimants' Request for Further Information dated 8 March 2018 ("**Dr Lynch's RFI Response**")). This does not make sense to me. I do not understand why customers who are said to have been given the flexibility to take their archiving solution in-house would have been more likely to sign up for longer term arrangements. In any event, customers who owned a Digital Safe licence and wanted to move out of Autonomy's data centre remained dependent on Autonomy for implementing Digital Safe either on-premise or in a third party's data centre. Autonomy would thereafter be involved in providing the ongoing managed services for Digital Safe and providing updates to the software. So even though a customer could in theory use its licence to switch provider, Autonomy would necessarily need to remain in the picture; the only difference would be that there would be another organization in the mix to provide the data centre where the data would be stored. Owning a licence to the Digital Safe software did not enable customers to run their archives entirely independently of Autonomy.
21. Dr Lynch says that the licence model *"offered [the customer] protection against the risk of rate increases when hosting arrangements came to an end"* (paragraph 139, LADCC). Hosting arrangements involving the sale of a licence still included a storage element and I cannot see what contractual guarantee against storage rate increases a licence gave customers that did not exist under a SaaS model. Perhaps Dr Lynch's suggestion is that if Autonomy increased its storage charges the customer could use the licence to host the

data itself without recourse to Autonomy. As I have explained, this was not a realistic alternative for the customer.

Building and running Digital Safe on a customer's premises

22. It was relatively unusual for a customer to have Digital Safe operating on-premise. Digital Safe was developed as a hosted offering and there were added difficulties if it sat somewhere other than in Autonomy's data centres. Autonomy needed to ensure that it could provide the same service to its on-premise customers that it did to its hosted customers. In practice, this meant that whenever Digital Safe was sold on an on-premise basis, Autonomy staff customised, configured and implemented Digital Safe on-premise on behalf of the customer and subsequently provided the necessary managed services through a remote virtual private network ("**VPN**") connection and/or by stationing Autonomy individuals to the customer's premises. Dr Lynch and Mr Hussain were aware of the failure with Rand (see paragraph 25(i) below) and consequently the need for Autonomy to be providing managed services. If a customer requested an on-premise Digital Safe set up, we would in the first instance ensure that such a set up was strictly necessary. We would check that there was a valid reason why: (a) our hosted Digital Safe offering; and (b) our on-premise archiving solutions (for example, EAS and CAMM), were unacceptable.
23. As regards implementation of Digital Safe, Dr Lynch says that "*Many companies themselves installed... Digital Safe*" (paragraph 48.4.3, LADCC). To my knowledge, there was not a single instance in the period 2008 to 2011 of a customer licensing Digital Safe software and then configuring and implementing a Digital Safe system on its premises itself. This was always done by Autonomy. As regards the ongoing operation of Digital Safe, Dr Lynch says that "*Many companies themselves... operated Digital Safe*" (paragraph 48.4.3, LADCC). Whilst some customers used their own / third party data centres to physically store their data, they did not operate Digital Safe without Autonomy. As I explain at paragraph 25 below by reference to specific on-premise customers, Autonomy always provided managed services when Digital Safe sat on a customer's premises.

On-premise customers

24. While on-premise Digital Safe customers hosted their data outside of Autonomy's data centres, they did not use Digital Safe "*independently of Autonomy*" (paragraph 154.1, LADCC) because they were reliant on Autonomy to provide the initial implementation services, followed by the 24/7 managed services.
25. I am not familiar with all of the on-premise customers that Dr Lynch refers to at paragraphs 153 and 154 of the LADCC, but I address below those which I am familiar

with. For all of the customers I refer to who actually received Digital Safe on-premise, Autonomy provided the initial implementation services to get the system up and running.

- (a) American Express. I recall that American Express' data was hosted in IBM's data centres. Autonomy provided the managed services for Digital Safe remotely via a VPN connection.
- (b) AXA. AXA was an on-premise Digital Safe customer. I do not think that AXA technically purchased managed services under its contract, but I am sure that Autonomy did in fact provide these services. On 11 March 2011, Stéphane Raszewski (Services Manager at Autonomy France) emailed me (amongst others) saying: *"Axa Im refused remote access to Digital Safe for security reasons although they might accept some exceptions (for support for example). I understood from the call we had with Roger last Wed that it is our interest for the Digital Safe to work/be operated properly that we obtain remote access for troubleshooting, maintenance, upgrade and most likely monitoring"* {D001141698}. The reference to Roger is a reference to Mr Wang. On 4 April 2011, Mr Raszewski emailed me (amongst others) again saying: *"I am pushing Axa Im to grant remote access. They seem to start accepting it but request in first place details on conditions... If Axa Im still refuses to provide Autonomy remote access to the environment for monitoring, troubleshooting or support activities then they will need to return the Digital Safe kit to Cambridge. I believe in the event Axa Im requests it, I should confirm that Autonomy doesn't provide Knowledge Transfer for customers to monitor, operate or troubleshoot Digital Safe themselves"* {D001025399}. We did not offer training to customers to enable them to monitor and operate (or indeed implement) Digital Safe themselves. Autonomy needed to provide these services, which is why we insisted that AXA accept our remote managed services.
- (c) BNP Paribas. BNP Paribas was an on-premise Digital Safe customer for which Autonomy provided managed services via a VPN connection. I recall that BNP Paribas entered into a Managed Services Agreement with Autonomy.
- (d) Citadel LLC. Citadel is, and always has been, a hosted Digital Safe customer.
- (e) Citibank. Citi used an on-premise hybrid of EAS and Digital Safe that was called First Archive. Citi ran the EAS component itself but Autonomy ran the Digital Safe component on a managed services basis through a VPN connection.
- (f) Deloitte. I do not recall Deloitte being an on-premise Digital Safe customer. If it had been, I think I would have known about it given my role.

- (g) Manufacturers Life. Digital Safe sat on-premise in Manufacturers Life's data centres and was managed remotely by Autonomy via a VPN connection. The transaction pre-dated Autonomy's data centre presence in Canada and Canadian law mandates that data must be hosted within the country. When Autonomy opened a data centre in Canada, Manufacturers Life moved its data there to become a hosted Digital Safe customer. On 6 September 2009, Brian Weiss (VP, Product Marketing) sent an email to George Tziahanas (VP, Compliance) and Alan Turner (VP, Product Management), which Mr Weiss subsequently forwarded to me, saying: *"we understand that supervisor and indeed DS to an extent is not well suited to onsite client management at this point. What we are saying is simply that we can't be competitive in this deal w an annual mgt fee roughly the equivalent of 2 FTE. So we either have to price it to be competitive and invest to make it work, or price ourselves out (ie walk away from the onsite DS+supervision market for now)... (Patrick is trying hard to get them to go hosted, but they are Canada based...)"* {D003719586}. Given the level of ongoing involvement from Autonomy in the running of Digital Safe, our standard and much preferred approach was for the safe to sit in Autonomy's data centres.
- (h) Merck. Merck was an on-premise Digital Safe customer for which Autonomy provided managed services via a VPN connection. I recall that Merck was concerned about the price of Autonomy's managed services and wanted to support Digital Safe itself without Autonomy providing any monitoring or operational support. On 27 November 2009, Claus Blank (Account Manager) emailed me (amongst others) saying: *"Sylvia needs asap the overview, what they need to do to maintain our appliance solution... Merck's expectations for operating an appliance are based on their experience with other appliances. There they only need to install patches, but are not responsible for keeping the OS alive, virus scanning"* {D003367289}. Al Martin (Technical Specialist Manager) responded explaining that Autonomy's *"Remote administrator provides full monitoring and administration of the system. This includes both the Autonomy software and Operating [sic] system. i.e. the appliance. It negates the need for Merck Operation staff to have to touch the inside of the boxes, only supplying power and cooling. Typical tasks include monitoring components are running, updating OS & software as needed, weekly/monthly/annual maintenance tasks (compactons etc)"* {D003367290}. We insisted on providing managed services to Merck.
- (i) Rand. Rand was authorised to sell Digital Safe to its own customers on a hosted basis. Autonomy sold Rand a licence to Digital Safe without managed services. However, Rand was unable to implement Digital Safe or run it on behalf of its customers so Autonomy licensed it "ACA" instead. ACA stood for Autonomy

Consolidated Archive and was used as an umbrella term for various archiving solutions. It was most likely EAS beneath the label.

- (j) SFO. The SFO was an on-premise Digital Safe customer. I remember that its contract failed to include managed services. This was because Autonomy sales representatives sold the SFO Digital Safe on-premise with no input from the technical team. In practice, Autonomy ran the SFO's safe and provided managed services: certain Autonomy employees had VPN access and there were a number of Autonomy individuals positioned on-site at the SFO.
- (k) UBS. UBS was an on-premise Digital Safe customer and Autonomy provided managed services through a VPN connection. In addition, Autonomy individuals were frequently stationed on-site at UBS to service Digital Safe. On 6 June 2011, I sent the UBS proposal to Mr Desroches and Hasan Imam (an Autonomy Client Director) and Mr Imam responded: "*I thought we stopped doing onsite DS...if onsite then CAMM?*" {D000690165}. It is not surprising to me that by 2011, Mr Imam thought we had stopped offering Digital Safe on-premise. Providing remote managed services and sending individuals on-site certainly created added difficulties that did not exist with the hosted offering.
- (l) VA Vaco. I primarily think of VA Vaco as having been an on-premise EAS customer but my understanding is that it also had on-premise Digital Safe. Autonomy provided managed services for Digital Safe over a VPN connection.

Re-restructuring transactions with Morgan Stanley, Deutsche Bank and Metropolitan Life

- 26. I have been referred to paragraphs 106A to 106AJ of the Claimants' (draft) Re-Re-Amended Particulars of Claim (the "**RRAPoC**"), which set out the various Digital Safe restructuring deals with Morgan Stanley, Deutsche Bank and Metropolitan Life. Although I only had limited direct involvement with these restructures, I remember hearing discussions about them at the time, and, with the benefit of having read the relevant parts of the RRAPoC, I will set out my views and impressions of the transactions below.
- 27. Following each of the restructures I describe below, Morgan Stanley, Deutsche Bank and Metropolitan Life received the same service as they would have done had they contracted on the SaaS basis; their data continued to be hosted in Autonomy's data centres. I do not think any of these customers intended to take Digital Safe on-premise and make use of the licences they had acquired. Rather, I think that they were keen to make savings and that Autonomy offered them this opportunity by significantly reducing their storage rates in return for licence purchases. Autonomy restructured Morgan Stanley's, Deutsche Bank's and Metropolitan Life's hosting arrangements not just once but twice, and three times in the case of Morgan Stanley. The incidental commercial

advantages for Autonomy of a restructure, such as they were, (e.g. enhanced customer retention and upsell opportunities) had already been obtained on the initial restructure. I cannot see any commercial justification beyond revenue recognition for re-structuring these customers' arrangements to reduce their storage rates even further – I believe the re-restructurings simply reflected Autonomy's desire to recognise more upfront revenue. On the subsequent restructures, Autonomy licensed new software that I believe was thrown in solely to differentiate the software from that which had been licensed previously to enable Autonomy to justify an additional licence fee.

Morgan Stanley

28. On 30 June 2008, Zantaz entered into an agreement with Morgan Stanley (the "**First MS Restructured Agreement**", {D000325148}) under which Morgan Stanley paid \$18.5 million for a perpetual licence to (amongst other things) version 8 and version 7.1 of the Digital Safe Archive System. On 31 December 2009, Zantaz entered into a further agreement with Morgan Stanley (the "**Second MS Restructured Agreement**", {D000352039}) under which Morgan Stanley paid \$12 million for another perpetual licence to the same software licensed under the First MS Restructured Agreement, with the addition of "SPE basic" within version 8 of Digital Safe. On 31 March 2011, Zantaz entered into a further agreement with Morgan Stanley (the "**Third MS Restructured Agreement**", {D001031127}) under which Morgan Stanley paid \$5 million for another perpetual licence to the same software licensed under the First and Second MS Restructured Agreements, as well as version 9 of Digital Safe (including "*Structured Data Load Capabilities, as provided by FileTek StorHouse/RFS and StorHouse/RM Software*"), DS Mail, ACA, Autonomy Social Media Connect and Supervisor (S6).
29. Under the Second MS Restructured Agreement, Morgan Stanley licensed SPE Basic as part of version 8 of Digital Safe for \$12 million. This makes no sense at all. To the best of my knowledge, SPE was never integrated with Digital Safe, so it was worthless to Morgan Stanley in this context – SPE's analysis functionality was never exposed within Digital Safe. I have been shown the Deloitte working paper setting out the justification for the transaction (as provided by Autonomy to Deloitte), which states: "*What the addition of SPE allows MS to do is to sort and archive all of their structured data from their transactional databases i.e. the databases that the bank uses to manage its customer accounts, value its numerous financial products and manage its finances. Given the volume of structured data held by MS globally, by purchasing DS with SPE, MS has significantly increased the amount of its data that can be archived in accordance with regulatory requirements*" {POS00141192}. The statement that SPE allowed Morgan Stanley to archive structured data from its transactional databases is incorrect. Digital Safe was already able to ingest structured data; its drawbacks were with subsequently analysing and searching the structured data in a useful way. In theory, SPE could have

offered that searching functionality, had it been integrated with Digital Safe. I am not entirely sure what is meant by the ability to "sort" structured data, but I should make clear that SPE was an analysis tool and nothing more. The statement that SPE allowed Morgan Stanley to sort and archive structured data from *"the databases that the bank uses to manage its customer accounts, value its numerous financial products and manage its finances"* is odd because I do not think that the core financial system that runs a bank account would be archived in Digital Safe. I also disagree with the statement that *"MS has significantly increased the amount of its data that can be archived in accordance with regulatory requirements"*. If data needed to be archived to satisfy regulatory requirements, it would have been archived irrespective of the presence of SPE. Further, I am not aware of Morgan Stanley ever making a considered effort to archive its structured data into Digital Safe.

30. Under the Third MS Restructured Agreement, additional software was licensed for \$5 million but again some of the additions do not make any sense to me. Morgan Stanley purchased a licence to Digital Safe version 9. First, I do not think that customers were generally expected to pay extra for upgrades to newer versions of Digital Safe, at least if the new version provided like-for-like functionality (in which case it would be provided free of charge). Software upgrades were covered by the maintenance and support fee (described at paragraph 10 above) attaching to the Digital Safe licence. In any event, version 9 did not exist at the time; it was only created in 2014. The day before the Third MS Restructured Agreement was signed, on 29 March 2011, James Crumbacher (of Autonomy's legal team) emailed me and Fernando Lucini (Chief Architect at Autonomy), copying in Michael McCarthy (Contracts Manager), saying: *"Chris, Fer, is there a version 9 of the Safe? Need it for Morgan Stanley (8.0 won't work), and Michael's telling me there's no v.9 on Automator. If Ver 9.0 exists, can we get it up on Automater for delivery?" {D001055839}*. I believe that Mr Crumbacher said *"8.0 won't work"* because Autonomy had already sold Morgan Stanley a licence to Digital Safe version 8 in June 2008, so would not have been able to license it again and recognise the revenue. I knew that version 9 did not exist, but Mr Lucini agreed to put a reference to version 9 on Automater and "deliver it" to Morgan Stanley. I assume that he understood the rationale for the transaction and Autonomy's need to add in new software to enable further upfront revenue recognition.
31. Digital Safe version 9 was said to include *"Structured Data Load Capabilities, as provided by FileTek StorHouse/RFS and StorHouse/RM Software"*. As I explain in further detail at paragraphs 74 to 78 below, the StorHouse software was not integrated with Digital Safe.
32. Morgan Stanley was already using Supervisor S6 and DS Mail before it entered into the Third MS Restructured Agreement. After the restructure, Morgan Stanley continued to receive the same service in respect of these applications. There were no advantages to

Morgan Stanley in owning licences to the applications; Supervisor S6 and DS Mail linked with and attached to Digital Safe so customers could not make use of them without Autonomy's managed services.

33. I am not sure why Morgan Stanley would have licensed ACA. ACA was a marketing term used to describe a range of Autonomy's archiving products (Digital Safe included).

Deutsche Bank

34. On 21 May 2008, Zantaz entered into an agreement with Deutsche Bank (the "**First DB Restructured Agreement**", {D002643998}) under which Deutsche Bank paid \$5.2 million for a licence to the Digital Safe Software. On 31 March 2011, Zantaz entered into a further agreement with Deutsche Bank (the "**Second DB Restructured Agreement**", {D001037832}) under which Deutsche Bank paid \$7.1 million for a licence to the same software licensed under the First DB Restructured Agreement, the only new software being version 9 of the Digital Safe Software with "*IDOL dense cell implementation*".
35. My views on the sale of Digital Safe version 9 to Deutsche Bank in March 2011 are the same as my views on the sale of Digital Safe version 9 to Morgan Stanley in March 2011; we could not legitimately have delivered version 9 in 2011 as it did not then exist.
36. Deutsche Bank also licensed "*IDOL dense cell implementation*". This, too, is very odd. Over time, as technology improved, Autonomy updated its hardware and storage cells. When this happened, cells usually became "denser" and this reduced the cost to Autonomy of storing data. Buying and implementing dense cells was an Autonomy overhead – the benefits derived from dense cells were only felt by Autonomy (through a reduction of its internal costs). It was not a piece of software that was licensed to clients. In any event, IDOL dense cells were incompatible with Lucene-powered safes, for which there were Lucene dense cells. Deutsche Bank is, and always has been, a Lucene safe customer. Dr Lynch states that "*Deutsche Bank expressed concerns over the performance capabilities of their Lucene Safe both before and after the execution of the Amended Agreement. In February 2011, Deutsche Bank and Autonomy discussed switching Deutsche Bank from a Lucene safe to Digital Safe*" (paragraph 149.5A.11, LADCC). I understand the second sentence to mean "*from a Lucene safe to an IDOL safe*". I recall that at one stage Deutsche Bank expressed a desire to move to an IDOL safe. However, I do not recall that this was due to concerns over the performance capabilities of Lucene; rather, Deutsche Bank felt that it should be using Autonomy's flagship product, which is how IDOL safes were marketed. I was not involved in all the discussions but I remember that Deutsche Bank expected to "upgrade" to IDOL for free and I expect that it would have been put off by the costs involved in making the transition. As far as I am aware, Deutsche Bank never switched to an IDOL safe so Autonomy could not have

used IDOL dense cells in connection with Deutsche Bank's Digital Safe storage needs. On 28 March 2011, Robert Mark emailed me saying: "*Chris, as we discussed, the software description now includes 'IDOL dense cell implementation (included in Digital Safe Software)'. There are no other references regarding what it includes, and no time lines associated with it*" {D001066031}.

Metropolitan Life

37. On 30 June 2010, Autonomy entered into an agreement with Metropolitan Life (the "**First ML Restructured Agreement**", {D002316492}, {D002352566}) under which Metropolitan Life paid \$7,025,000 for a licence to (amongst other things) the Digital Safe Archive System Software (for use with up to 40,000 users). On 30 June 2011, Autonomy entered into a further agreement with Metropolitan Life (the "**Second ML Restructured Agreement**", {D000488076}) under which Metropolitan Life paid \$5.5 million for a licence to the same software licensed under the First ML Restructured Agreement, with the addition of the "*Discover Engine*" connector.
38. I have been shown a description of Discover Engine {D010858864}. Discover Engine looks to be a connector that extracts and indexes SharePoint data. I know that Autonomy already had a SharePoint connector called Autonomy SharePoint Connector. Dr Lynch states: "*Autonomy's SharePoint connector, ControlPoint, was primitive by comparison and was not Microsoft certified. Additionally, DiscoverEngine supported data encryption, which Autonomy's ControlPoint did not have at this time*" (response 55, Dr Lynch's RFI Response). Dr Lynch also states: "*DiscoverEngine's functionality interfaced with a range of compliance products, including Autonomy Legal Hold and Autonomy Consolidated Archive Hold*" (response 56, Dr Lynch's RFI Response). I should make clear that ControlPoint is a SharePoint related application but is not itself a connector. Much of the functionality that Dr Lynch says Discover Engine provided was also provided by Autonomy SharePoint Connector: (i) Autonomy SharePoint Connector supported data encryption; and (ii) Autonomy SharePoint Connector could interface with compliance products including Autonomy Legal Hold and Autonomy Consolidated Archive Hold – Autonomy sold Autonomy SharePoint Connector to customers who needed both the Legal Hold and SharePoint functionality. Mr Hussain states that "*MLIC was not simply a Digital Safe customer. So far as Mr Hussain is aware, it also licensed, for example, Autonomy's Aungate Investigator and ECA software, which could be used with DiscoverEngine*" (paragraph 233AH(d)(3), HAD). Autonomy SharePoint Connector could interface with those products too. If Metropolitan Life had needed a SharePoint connector, I see no reason why it would not have been sold Autonomy SharePoint Connector.

39. I am not familiar with Discover Engine beyond the description I have been shown. If Discover Engine had functionality that went beyond what Autonomy SharePoint Connector offered, I expect that Autonomy could have built or developed that additional functionality fairly easily had it been desired.
40. I have been told that Autonomy provided Deloitte with the following justification for its purchase of Discover Engine from Discover Technologies LCC (which was consequently reflected in Deloitte's report to the Audit Committee for the H1 2011 Interim Review {POS00171419}): *"During Q2 2011 Autonomy purchased a \$4.4 million perpetual reseller licence from Discover Technologies LLC for their product DiscoverPoint. This purchase was made such that Autonomy could complete a number of IDOL based licence revenue sales with Bloomberg, National Bank of Canada and MetLife, who all required the advanced Microsoft SharePoint connectivity provided by the DiscoverPoint product and not currently offered by the Autonomy products they were purchasing."* I can think of no reason why, if Bloomberg, National Bank of Canada and Metropolitan Life required a SharePoint connector, Autonomy Sharepoint Connector would not have done the job. I am surprised that Autonomy purchased Discover Engine for \$4.4 million given Autonomy's general reluctance to buy any third party software. Autonomy's philosophy with regards to third party software was well known within the company. Typically, Autonomy did not buy third party software unless there were no alternative. Instead, it would, wherever possible, develop any software that it required internally.
41. I have been provided with a selection of emails (to which I am not a party) which appear to explain how Discover Engine came to be included in the Second ML Restructured Agreement. On 17 June 2011, Ivan Rothman (Autonomy Senior Corporate Counsel) emailed Robert Sass (an Autonomy salesperson) saying *"... I understand we now need to add Share Point Connector to both this document and the Bloomberg document – correct?"* {D000625607}. Mr Sass responded: *"sorry, no clue what you are talking about."* {D000625747}. Mr Rothman responded *"My understanding is that Sush has decided we should give this connector to MetLife and Bloomberg (for free) as a way to promote this product."* {D000625606}. Mr Sass replied: *"Let me call Sush."* {D000625749}. Later that day, Mr Rothman emailed Mr Sass saying: *"I added the language Sush requested re the connector (actually called DiscoverEngine", not "SharePoint")."* {D000625594}. It appears that there was a general push at the time from Mr Hussain to add Discover Engine into various customer contracts for free, to show that Autonomy had made "sales" of Discover Engine. I have been shown an email dated 17 June 2011 in which Mr Crumbacher emailed Joel Scott (General Counsel at Autonomy) saying: *"FYI, information on the product to be inserted into MetLife, Tracfone, National Bank of Canada, and Bloomberg... since Sushovan asked you, personally, to come up with the customers and*

since I don't know what criteria were given in choosing them, I'll follow your lead."
 {D000620736}

Video Monitoring Services of America, LP Q2 2009 transaction

42. I understand that, on 30 June 2009, Autonomy Inc purchased a licence from VMS LP to use VMS's data feed and display VMS's data for three years for \$13 million {D003997524}. As far as I recall, I did not have any involvement in this particular transaction, nor was I aware of it at the time.

VMS's data feed

43. For a number of years up until 2009, Autonomy received a news feed (a mechanism which pulled data from various news outlets) which was provided free of charge by Moreover Technologies, Inc ("**Moreover**"). This news feed was primarily used by Autonomy in its demonstration environment. In June 2009, Moreover informed Autonomy that it was no longer willing to provide its data feed to Autonomy free of charge and offered instead to license the feed to Autonomy for £50,000 per annum {D003920940}. Rather than incurring that cost, Autonomy decided to develop its own data feed, which would replace Moreover's news feed.
44. On 20 July 2009, I received an email from Dr Menell, which tasked me, Sean Blanchflower (Head of Research & Development at Autonomy) and Mr Lucini with the development of an Autonomy data feed {D003920940}. This was to be completed by 31 July 2009, which was when the Moreover data feed would be switched off if we did not agree to pay their proposed fee. Dr Menell's email forwarded on an email he had sent to Mr Hussain, in which he made plain that paying £50,000 per annum for the Moreover data feed was unacceptable: *"So renewing Moreover would be something we would do if a) we were lazy and have been lazy b) we ever listened to humans calling themselves "product managers". Thus time to bite that bullet and package our own that given our technology will utterly obliterate the likes of Moreover"*. Mr Lucini replied to Dr Menell's email stating: *"Sean has been working on this since we had the first service cut"* {D003920941}. I understand this to refer to a cut in the Moreover feed in June 2009. Dr Blanchflower duly completed the feed he had been working on, which was used to replace the Moreover feed in our demonstration environment. When I left HP/Micro Focus in February 2018, it was still using this data feed for its demonstrations.
45. I have been shown a copy of the Project Shockwave Business Plan (the "**Business Plan**") {POS00131231}. The Business Plan stated that Autonomy wanted to acquire VMS's data feed in order (i) to integrate it into its Interwoven product suites; and (ii) to use it in Autonomy's demonstration environment. At the time, I was not aware of and did not see the Business Plan nor had I heard of the code name "Project Shockwave".

46. In my opinion, neither of these supposed uses for the VMS feed justified its purchase by Autonomy at a cost of \$13 million. I am not aware of the VMS feed being used for either of these purposes. I do not, therefore, see any genuine business case for Autonomy buying it.

Q4 2010 VMS transaction

47. I understand that, on 31 December 2010, Autonomy Inc purchased from VMS LP additional rights to VMS's data feed for \$8.4 million ("**VMS Purchase 2**") {D001451566}. I was not aware of VMS Purchase 2 at the time, which makes no more sense to me than the first VMS purchase referred to above.
48. Also on 31 December 2010, Autonomy Inc sold hardware to VMS Inc for \$6,004,067 million ("**VMS Sale 2**") {D006127170} and sold software licences to VMS LP for \$5 million (\$4.75 million for the software licence fee and \$250,000 for one year's support and maintenance) ("**VMS Sale 3**") {D001451567}. I was aware of these two transactions at the time and, as explained below, was closely involved in the hardware sale.

VMS's purchase of hardware from Autonomy – VMS Sale 2

49. In around mid-December 2010, Dr Menell asked for my assistance in relation to VMS Sale 2. I was tasked with: (1) finding out what hardware VMS wanted; (2) exploring how much it would cost Autonomy to purchase that hardware from a third party supplier; (3) discussing with VMS what it was prepared to pay for the hardware; and (4) arranging for the hardware to be ordered and delivered to VMS. I believe that Dr Menell asked for my assistance due to my experience of purchasing hardware for Autonomy's internal use in relation to its Digital Safe business or for on-sale to customers as an appliance with Autonomy's software pre-installed on it. When Autonomy needed to purchase hardware for these purposes, it was not uncommon for me to be involved.
50. Before VMS Sale 2, I believe the largest sale of hardware to a customer with which I was personally involved was in the region of approximately \$200,000 to \$250,000. Autonomy's sale of \$6 million worth of hardware to VMS was certainly significantly larger than any other hardware sale with which I had previously been involved.
51. On 17 December 2010, Dr Menell forwarded to Poppy Prentis (Corporate Financial Controller at Autonomy) and me an email which he had received from Christopher (Stouffer) Egan (CEO of Autonomy Inc.), attaching the hardware specifications for VMS Sale 2 {D001509536}, {D001509537}. VMS's preferred hardware was HP hardware. I sought quotes from HP, as well as from Dell and for "white-label" hardware (non-branded hardware) (see, for example, {D001508609}). When seeking a quote, I did not contact HP directly. Instead, I dealt with Insight Direct (UK) Limited ("**Insight**"), a UK

reseller of HP hardware (which bought hardware from HP and then resold it to end-users). We used Insight rather than a US reseller (notwithstanding that VMS was based in the US) because Autonomy had an existing relationship with Insight which would make it easier to negotiate the purchase within the tight timetable set. Prior to HP's acquisition of Autonomy, Autonomy did not purchase much HP hardware. Autonomy typically purchased as "white label" hardware for its own internal use or for use as an appliance (a combination of hardware and software delivered together).

52. On 20 December 2010, Mr Egan put me in touch (by email) with Gerry Louw (VMS's Chief Information Officer) {D001501448}, which allowed me to liaise directly with VMS to determine what its hardware needs were, and how we could meet them (see, for example, {D001501575}, {D001501576}). Initially, I tried to buy all of the hardware from HP (via Insight), as can be seen from my email to Nicole Eagan (Chief Marketing Officer at Autonomy) and Eloy Avila (CTO of Autonomy, Inc) on 23 December 2010 {D001481096}, {D001481097}.
53. VMS wanted flexibility in relation to the specification of the hardware it was to buy {D001473219}. It appeared to me that VMS had a budget to spend and that it had created a "wish list" of hardware that would fit within that budget, as opposed to identifying hardware that it needed and negotiating the best price for that. It also seemed to me that VMS was not entirely sure what hardware it wanted to buy. It wanted the flexibility to make changes to its hardware order after 31 December 2010. In view of the significant purchase price, I would have expected VMS to have had a business plan setting out a use case for the purchased hardware, and for the purchase to have been planned by it for some time. The fact that VMS kept changing its hardware order gave me the impression that there had been little planning by VMS as to what hardware it required or wished to purchase.
54. VMS Sale 2 was negotiated very quickly, which was also unusual for a transaction of this size. My sense was that VMS entered into this transaction more quickly than it would otherwise have done in order to meet Autonomy's need for it to take place in Q4 2010. It was well-known throughout Autonomy that Autonomy was quarter driven and there was always significant sales activity towards the end of a quarter.
55. On 31 December 2010, I sent an email to Dr Lynch, Mr Hussain and Dr Menell seeking approval for the purchase order to Insight for \$5,846,546.65 worth of HP hardware {D001452860}. In my email, I explained that "*We are still negotiating final pricing so this is likely to improve however in order to bond the stock we need to issue the PO this evening. Please approve*". Dr Lynch approved the purchase order that day {D001453776}, as did Dr Menell {D001456967}. Mr Hussain commented on 31 December 2010, "*FYI we are buying the hardware*" {D001453796}.

56. Later that evening, Mr Hussain asked whether there was *"any hardware we can repurpose?"* {D001453796}. At the time, this struck me as an odd request, as I had been negotiating with Insight and VMS for several days on the understanding that VMS wanted HP hardware which would be purchased from Insight.
57. Richard Eads, who was Head of Procurement at Autonomy, forwarded Dr Lynch's approval to Mr Hussain and explained that Mr Hussain's approval was also required before he could proceed with the purchase of HP hardware from Insight {D001456730}. Mr Hussain responded to Mr Eads (Mr Hussain also sent his response to me and Dr Menell) stating: *"Not yet still working out the number we can repurpose from stock. Will get back to you in a while"* {D001453793}. It was clear to me that Mr Hussain wanted to know if Autonomy had any hardware in its internal stock that it could use to fulfil VMS's hardware order. Dr Menell subsequently asked me to obtain a copy of Autonomy's fixed asset register, review it, and determine whether any of that hardware was similar to that which we were proposing to sell to VMS (regardless of age, brand or location and whether or not the hardware was already in use).
58. On 31 December 2010, in response to a request from Ganesh Vaidyanathan (Director of Accounting at Autonomy), Huaimin Ding (Senior G/L Accountant at Autonomy) sent me and Mr Vaidyanathan (copied to Mr Chamberlain) a copy of ZANTAZ's US fixed asset register as at that date {D001453825}, {D001453826}. I used that register to create a list of hardware already owned by Zantaz which was similar specification to the hardware that VMS wanted ({D001451047}, {D001451048}, {D001451049}). The list I created included hardware that was presently being used by Autonomy for its own internal purposes, hardware that had been obtained for delivery to a customer, and hardware that was not yet in use (i.e. that was still sitting in boxes). This was all very peculiar. The "used" hardware was unlikely to be of the latest specification and it may well have held confidential data belonging to other customers. The customers who own that data would, very likely, not want the hardware to be given to anyone else and would want the hardware to be destroyed if it was to leave our possession. As Autonomy management would surely have known, there is no way that VMS would have accepted "used" repurposed hardware – it's order was for new HP hardware.
59. On 31 December 2010, Mr Hussain sent a further email to Mr Eads stating, *"Speaking with pete [Peter Menell] and steve [Steve Chamberlain] I believe we are buying less circa 2m and repurposing the rest from existing stock. Spreadsheet being prepared"* {D001453792}. By this point I had not yet produced my list, but I understood Mr Hussain's instruction to be that only around \$2 million of HP hardware was to be purchased from Insight, and that the rest of VMS's \$6 million hardware order would supposedly be fulfilled from Autonomy stock. At the time, Autonomy did not have \$4 million worth of hardware sitting in boxes (i.e. not in use) for on-sale to VMS, so

fulfilment of VMS's order would necessarily have involved the repurposing of hardware that was already in use by Autonomy.

60. I subsequently sent Mr Eads an email on 31 December 2010 which attached Autonomy's updated purchase requirements from Insight, and provided confirmation that Autonomy was only going to purchase circa \$2.5 million of HP hardware, even though we had been negotiating with Insight for some time for the purchase of \$6 million worth of HP hardware {D001453857}, {D001453858}. Mr Eads responded later that day (copied to Mr Hussain), stating he had informed his contact at Insight of the last minute change to the deal, "*I think my contact at Insight UK just had a stroke. Trying to bring him back to life now*" {D001452875}. I took this to mean that his contact at Insight had been surprised and disappointed to learn that we intended to substantially reduce the amount of our order at such a late stage.
61. On the following day, 1 January 2011, I sent Mr Eads the list I had produced of inventory hardware that might be supplied to VMS, including hardware that was in use and was not in use {D001451047}, {D001451048}, {D001451049}. I then sent a follow-up email to Mr Eads which identified additional Autonomy hardware that was not in use {D001451050}.
62. To the best of my knowledge, the new HP hardware purchased from Insight was delivered to VMS. However, I do not believe that any of the repurposed Autonomy hardware was ever delivered. I was in communication with VMS in relation to the delivery of hardware (see for example {D001280281}, {D001223783}), but, surprisingly, while VMS did chase me, it did not do so as aggressively as I would have expected where it had only received about a third of the \$6 million worth of hardware it had bought.
63. The payment terms for VMS Sale 2 were unusually generous and were staggered across almost two years. Payment was due from VMS in four tranches, the first of which did not fall due for almost a year {D006127170} (see page 2).
64. In June 2011, VMS emailed me to ask whether Autonomy would consider buying back some of the hardware that VMS had purchased from Autonomy in VMS Sale 2 {D000578523}. VMS said it no longer needed the amount of hardware that it had bought and wanted to sell some of it back to Autonomy in order to fund "*another immediate opportunity*" at VMS {D000578523}. This discussion continued into August {D000327567}. On 10 August 2011, Mr Hussain sent an email to me and Mr Chamberlain, stating: "*need urgent chat re VMS*" {D000323071}. I believe I had a call with Mr Hussain to discuss a possible buyback of hardware from VMS and also the fact that VMS went bankrupt shortly after that.

65. VMS filed for bankruptcy in August 2011, so I believe that we never delivered the full \$6 million of hardware purchased by VMS. I do not know if Autonomy collected the hardware that had been delivered to VMS, (for which, I believe, VMS had not paid Autonomy as the first payment was not due until December 2011).

FileTek Inc ("FileTek")

66. On 31 December 2009, Autonomy Inc purchased licences for StorHouse software (and related support) from FileTek for almost \$10.4 million {FT 0000092}, {FT0002011}. In very simple terms, I would describe StorHouse as a database archiving product.
67. On 30 December 2009, Dr Menell forwarded to me an email from Mr Crumbacher attaching FileTek's draft agreement for Autonomy's proposed purchase of StorHouse, asking him to look at certain of its terms {D003238683},{D003238684}. Dr Menell forwarded the email to me, stating: *"Need this pass DS standards. Chris doing first pass"* (the reference to "DS" was to Digital Safe, one of Autonomy's digital archiving products). Dr Menell wanted me to check that the service level support for StorHouse was comparable to the service levels Autonomy provided to Digital Safe customers. I responded that day with my initial comments {D003238662} {D003238663}. By the time I received the draft agreement, the purchase price had already been agreed. My task was limited to checking that its technical terms were appropriate. On 31 December 2009, Mr Crumbacher sent a further email to me and Mr Egan asking us to review the product schedules to the StorHouse agreement to ensure that they accurately reflected the agreed business terms and matched our expectations and needs, e.g. whether the product schedules *"offer us [Autonomy] sufficient room to grow without having to buy additional licenses"* {D003234997}, {D003234998}, {D003234999}.
68. When I became aware of Autonomy's intended purchase of StorHouse, I was surprised, as it was an unusual transaction for Autonomy to enter into given its general reluctance to buy any third party software and the significant purchase price. I asked Dr Menell to explain the rationale for the transaction. He did not provide a satisfactory response, although that was not particularly surprising – we were used to Dr Menell keeping us in the dark in this way.

Autonomy's analysis of the StorHouse software

69. I have been shown a copy of an email dated 31 December 2009 from Dr Menell to Dr Lynch, Mr Hussain and others, in which Dr Menell set out Autonomy's justification for its purchase of StorHouse and Autonomy's analysis of the software {D003230356}, {D003230357}, {D003230358}. Dr Menell commented: *"The market case for the automatic software product that permits an enterprise to at once reduce its RDBMS license and hardware cost while maintaining regulatory compliant access to the original*

data is self evident and extremely compelling. This acquisition permits the rapid creation of such a unique product through combining FileTek technology with DS and SPE". Attached to Dr Menell's email was Dr Menell's technical memorandum on the product. I do not recall seeing either the email or the memorandum at the time.

70. The email and technical memorandum amounted to what is often described as a 'use case', in other words, a description of how the product could potentially be used. A 'use case' differs from a 'proof of concept', which would ordinarily be undertaken prior to a purchase. In contrast to a use case, which simply outlines the software's potential/an idea as to how the software could be used, a proof of concept involves a more detailed analysis and evaluation of the software to confirm that it can be utilised for its intended purpose and can be integrated with any existing software as required.
71. If a product was to be purchased with the intention of being used within the Digital Safe environment, given the oversight which I had of Autonomy's hosted offerings, I would have expected to have been involved in the analysis and testing of StorHouse, (along with others in Digital Safe's technical team). To the best of my knowledge, I understand that Autonomy did not carry out a proof of concept before it purchased StorHouse, or any of the detailed testing and analysis of the StorHouse software that I would have expected to ensure that it met Autonomy's requirements and in particular that it could be integrated with Digital Safe. This makes no business sense to me.

StorHouse demonstration in January 2010

72. In January 2010, I attended Autonomy's sales conference in Miami. This was an annual event, taking place typically at the beginning of the financial year, at which all Autonomy employees involved in selling products to customers would meet to discuss the sales teams' plans and aims for the year ahead. While I was at the conference, Dr Menell asked me to create a demonstration for Deloitte (in its capacity as Autonomy's auditors, rather than as a customer) of a use case for the StorHouse software. I do not recall Dr Menell providing me with a use case to demonstrate, so I had to come up with one myself.
73. I asked two colleagues, Tina Kim and Shane Connelly, a systems engineer and technology specialist respectively, to assist me with this task. We created a simple demonstration which showcased StorHouse's functionalities rather than the StorHouse software itself – we had not installed the StorHouse software at the time. I showed Dr Menell the demonstration and provided him with a copy of it, but I do not know what he did with it subsequently, nor whether it was provided to Deloitte.

Attempts to integrate StorHouse with Digital Safe

74. I was part of the team which attempted to integrate StorHouse with Digital Safe. As at April 2010, we were still struggling with the installation of StorHouse, as can be seen from the emails dated 1 April 2010 that I exchanged with Darren Gallagher (Head of Development at Autonomy), who was also involved in the process {D002807543}. On 16 April 2010, Jonathan Hayman (an Autonomy employee), who was also part of the team attempting to integrate StorHouse and Digital Safe, sent an email to Mr Gallagher confirming that he had finally installed the StorHouse software {D002744924}.
75. Later that month, on 30 April 2010, Mr Egan sent an email to Dr Menell and me attaching a proposal for the purchase of additional StorHouse capacity {D002677551} {D002677552}. In his email, Mr Egan commented: *"This is Filetek's first proposal for the additional volume we asked about as a result of our winning the Merrill Lynch, MetLife and Newedge deals. They don't know about Lily volume, BNPP, The new larger JPMC volumes and the rate at which volumes are growing. Either way we need at least this much moiré [sic] and we need a negotiation strategy to get further discount"*.
76. Although it was sent to me, I do not remember considering this proposal at the time. As I look at it now, though, it does seem very odd. Under the 31 December 2009 agreement, Autonomy licensed StorHouse for up to 60 customers capped at 10 petabyte of file data and 1 petabyte of structured data over a five year term {FT0002011}. Under the April 2010 proposal, FileTek offered to licence StorHouse to Autonomy without capacity restraints. At that time, however, we had only just installed the StoreHouse software and were in the very early stages of our attempts to integrate it with Digital Safe. We had not sold it to any customers and hadn't used any of the capacity that we had paid over \$10 million for in December 2009. In those circumstances, I can think of no reason to propose buying additional capacity in April 2010.
77. I understand that, on 11 May 2010, Autonomy proceeded with its purchase of additional StorHouse capacity from FileTek at a cost of \$11,518,214 {POS00158260}, {POS00158261}. This makes no more sense to me than the April 2010 proposal. I understand from the Claimants' solicitors that Mr Wang is giving a Witness Statement which contains a detailed description of our attempts to integrate StorHouse and Digital Safe, which I will not repeat here. However, I confirm that, as at mid-May 2010, we were still looking at ways in which we might perform the integration (see for example {D002600066}). We had not used any of our existing StorHouse capacity so had no need for additional capacity. As far as I am aware, despite these efforts, we never successfully integrated the StorHouse software with Digital Safe in such a way that we had a commercially saleable product. Nor am I aware of it ever being used to provide any benefit or value to Autonomy or its customers.

78. I understand from the Claimants' solicitors that Mr Wang describes in his Witness Statement setting up an instance of StorHouse in Kraft's production safe and explains how Autonomy addressed Kraft's structured data requirements, so I will not repeat that detail here. To the best of my knowledge, StorHouse was not used to address Kraft's or any other customer's structured data requirements. Inserting a piece of software into a customer's production safe i.e. a customer's main Digital Safe is relatively easy to do and does not mean that the software was sold to a customer or that the customer used the software. Deploying an instance of StorHouse in Kraft's production safe does not mean that StorHouse was successfully integrated in Kraft's production safe or that Kraft used StorHouse or that Kraft was even aware that it had an instance of StorHouse in its production safe.
79. During cross-examination in Mr Hussain's Criminal trial (the "**US Trial**"), I stated that there was basic integration between Digital Safe and StorHouse. What I meant by that was that StorHouse was installed on, and shared, the same hardware as Digital Safe within Kraft's production safe. There was not, however, any code integration and therefore nothing which delivered value to either Autonomy or Autonomy's customers. This is perhaps best illustrated by the analogy I gave in my re-direct examination in the US trial. We had a car (Digital Safe) and we purchased another engine (StorHouse) for that car. We put the engine in the car, but it was not connected and so did not provide any additional horsepower. The net result was a car that was actually slower than before as it now had to carry around not one but two engines.

Repurposing of EMC hardware

80. In October 2010, Autonomy was in discussions with JPMC regarding enhancements to the service that required additional hardware. On 7 October 2010, I sent an email to Dr Menell, copied to others, attaching an updated purchase order for \$556,162 in respect of hardware which Autonomy planned to purchase for JPMC {**D001834736**}, {**D001834737**}. The following day, Dr Menell replied, saying "*... still way to high given our investment in an EMC backbone. I do not believe that we cannot optimise further if necessary. Software can be changed and will be to take full advantage of EMC backbone*" {**D001829070**}. Dr Menell wanted to use hardware purchased from EMC in Q3 2010 for another purpose (the "**EMC Hardware**") to fulfil JPMC's hardware requirements. On 8 October 2010, I replied to Dr Menell setting out how much it would cost to use the EMC Hardware in comparison to purchasing new hardware {**D001829141**}. I told Dr Menell that the "*EMC option would be more expensive*" and I asked that he approve the purchase order for \$556,162. Dr Menell was insistent, though, on the use of the EMC Hardware and noted "*Chaps you misunderstand me. We don't want an "EMC option". We already have that option as we have made a large order to EMC. So we have all the EMC kit we need. So what we need is a architecture that takes advantage of that fact*"

and only gets the necessary processing power as we don't need to order anymore storage as this is already covered. The old model assumed we did not have the EMC equipment the new world means we don't have to use the same old architecture and we can build a new built mainly on EMC with some additional processing power popped on top. So this means this order should and can be a lot smaller" {D001823103}.

81. On 15 October 2010, I sent an email to Dr Lynch and Mr Hussain, seeking approval for the JPMC hardware purchase order in the sum of \$556,162 {D001800067}. I explained that if we used the purchased EMC Hardware (as Dr Menell wanted to), it would cost Autonomy a minimum of \$572,000, i.e. it would cost Autonomy more to use the purchased EMC Hardware for JPMC, than not to use it. Dr Lynch replied saying "*chris, pls go ahead provided you have had a call with sushovan to understand the emc kit we bought last quarter*" {D001798270}. I do not recall whether I spoke to Mr Hussain, as instructed to do so by Dr Lynch.
82. On 19 October 2010, Mr Gallagher sent an email to Messrs Wang, Avila and me in relation to the use of the purchased EMC Hardware {D001789135}. Mr Gallagher stated "*I just had Pete [Menell] on the line. He would like . . . b) A diagram that shows how we would achieve the below but using some/all of the EMC HW we just bought and hence we can reduce the spend form [sic] \$1.2m to say \$0.5m*". Mr Wang replied: "*Given the low cost of hard drives utilizing EMC will not save much as we'll still need the processing head units. In addition we will need to add a fiber card to each machine plus build out a fiber network in the datacenter. The initial feeling is that it will almost definitely increase not decrease cost*" {D001789143}. I replied setting out my thoughts on pricing {D010817600}. As Mr Wang said in his email, it was unlikely to be cost effective to use the purchased EMC Hardware to meet JPMC's hardware requirements given the cost of the additional hardware that we would have to buy to make the EMC Hardware fit for purpose.
83. I later became aware that Dr Lynch had given Dr Menell four days to review the position and determine whether the purchased EMC Hardware should be used for JPMC {D001789173}. I sent an email to Dr Lynch on 19 October 2010 noting this and setting out the three available options, one of which was based on the use of the purchased EMC Hardware {D001789173}. On 20 October 2010, Dr Lynch responded (copying in Dr Menell) saying "*sort it out between yourselves chaps*" {D001784134}. On 22 October 2010, I sent a further email to Dr Lynch asking that he call me at his convenience as I wished to discuss this matter with him {D001774540}. I recall having a four way conversation with Dr Lynch, Dr Menell and Mr Sullivan to discuss this matter further, but I do not recall the detail of the conversation.

84. On 25 October 2010, Dr Lynch sent an email to me, Dr Menell and Messrs Avila, Egan, Desroches and Sullivan in relation to the purchase of hardware for JPMC, saying *"Thankyou for you [sic] inputs on this which were all valid. There were many things to consider. Having taken into account all factors I have reached a conclusion on this and Pete and Chris will implement, it is the smaller EMC based approach"* {D001765641}. To my mind, this made no sense as it was more expensive for Autonomy to use the EMC Hardware for JPMC than to buy new hardware.
85. Following Dr Lynch's email on 25 October 2010, I recall having a conversation with him in which I asked why Autonomy intended to use the EMC Hardware when that was not the most cost-effective option. Dr Lynch replied with something along the lines of: *"You know when your parents tell you something as a child which you don't understand, this is one of those instances"*.

MicroTech / HP VAR transaction - The Federal Cloud Platform

86. I understand that, on 30 June 2011, Autonomy Inc received a purchase order from MicroTech for \$7 million (plus \$350,000 support and maintenance), which specified HP as the end-user {D000523485}. I also understand that on 15 August 2011, MicroTech and Autonomy Systems Limited ("**ASL**") entered into an agreement under which MicroTech was to develop a US Government Federal Cloud Platform (a "**Federal Cloud Platform**") for ASL at a cost of \$8.2 million {POS00399720}.
87. I was not aware of this transaction at the time. Given my involvement in Autonomy's cloud offerings and my daily role in Autonomy's SaaS business, I find it surprising that ASL entered into an agreement with MicroTech for the development of a Federal Cloud Platform without my knowledge or involvement, particularly for a sum as large as \$8.2 million. I was also unaware of any customer requirement for a federal cloud platform (and if there had been one I would expect to have known about it).
88. If Autonomy had a legitimate need for a federal cloud platform, I would have expected Autonomy, rather than MicroTech, to have developed one - Autonomy certainly had the capability to do it. As with the other transactions referred to above, outsourcing the development of a federal cloud platform to a third party went against Autonomy's philosophy of developing its own products and software internally.
89. I have been shown a copy of MicroTech's proposal for the development of a Federal Cloud Platform {D000318982}. I have also been shown a copy of an email dated 10 August 2011 from Mr Hussain to Dr Menell, Andrew Kanter (Chief Operating Officer and General Counsel at Autonomy) and Mr Scott, copied to Mr Egan and Dr Lynch, in which Mr Hussain explained that the Federal Cloud Platform would enable Autonomy to fulfil

its existing contract between Microlink LLC ("**Microlink**") (a subsidiary of Autonomy) and the Social Security Administration ("**SSA**") {**D000318981**}.

90. I understand from the Claimants solicitors that, on 12 May 2011, Microlink entered into an agreement with the SSA, under which Microlink was to provide an enterprise level email archive system, email records management and eDiscovery management to the SSA {**D000780551**}. I have been shown a copy of an email dated 20 May 2011 from Rajan Srivatsan (an Autonomy employee) setting out a "*brief description of the scope of the SSA E-mail Archive/E-mail Management/eDiscovery System*: • *SSA plans to deploy an onsite end-to-end Information Governance and eDiscovery solution that includes:* • *Email Archiving for 105,000 end-users using Microsoft Exchange, served by 4 data centers across the country* • *Email Records Management that is compliant with NARA regulations* • *eDiscovery Management that includes Legal Hold, Legal Search, Review & Production, for 800 users*" {**D000780551**}. These services did not require a Federal Cloud Platform. Based on the email above, the SSA agreement was for an on-premise offering. As such, Autonomy did not need a Federal Cloud Platform in order to fulfil the SSA agreement.

I believe that the facts stated in this Witness Statement are true.

Goodfellow

SIGNED

CHRISTOPHER JAMES ROBIN GOODFELLOW

14th September 2018

DATED

1.	On behalf of	Claimants
2.	Initials/Surname of witness	C J R Goodfellow
3.	Statement No	1
4.	Date	14 September 2018

Claim No. HC-2015-001324

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
BUSINESS LIST (CHD)

B E T W E E N:

**(1) ACL NETHERLANDS B.V. (AS SUCCESSOR TO
AUTONOMY CORPORATION LIMITED)**
(2) HEWLETT-PACKARD VISION BV
(3) AUTONOMY SYSTEMS LIMITED
(4) HEWLETT-PACKARD NEW JERSEY, INC

Claimants

-and-

(1) MICHAEL RICHARD LYNCH
(2) SUSHOVAN TAREQUE HUSSAIN
Defendants

**WITNESS STATEMENT OF
CHRISTOPHER JAMES ROBIN GOODFELLOW**

Travers Smith LLP
10 Snow Hill
London EC1A 2AL
Tel: 020-7295 3000
Fax: 020-7295 3500
Ref: TPR/AAK/JJB/SEL

1.	On behalf of	Claimants
2.	Initials/Surname of witness	C J R Goodfellow
3.	Statement No	1
4.	Date	14 September 2018

Claim No. HC-2015-001324

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
BUSINESS LIST (ChD)

B E T W E E N:

(1) ACL NETHERLANDS B.V. (AS SUCCESSOR TO AUTONOMY CORPORATION LIMITED)
(2) HEWLETT-PACKARD VISION BV
(3) AUTONOMY SYSTEMS LIMITED
(4) HEWLETT-PACKARD ENTERPRISE NEW JERSEY, INC.

Claimants

-and-

(1) MICHAEL RICHARD LYNCH
(2) SUSHOVAN TAREQUE HUSSAIN

Defendants

INDEX OF EXHIBITS TO THE
WITNESS STATEMENT OF CHRISTOPHER JAMES ROBIN GOODFELLOW

	Paragraph	Production ID
1	25(b)	D001141698
2		D001025399
3	25(g)	D003719586
4	25(h)	D003367289
5		D003367290
6	25(k)	D000690165
7	28	D000325148
8		D000352039

9	28	D001031127
10	29	POS00141192
11	30	D001055839
12	34	D002643998
13		D001037832
14	36	D001066031
15	37	D002316492
16		D002352566
17		D000488076
18	38	D010858864
19	40	POS00171419
20	41	D000625607
21		D000625747
22		D000625606
23		D000625749
24		D000625594
25		D000620736
26	42	D003997524
27	43	D003920940
28	44	D003920940
29		D003920941
30	45	POS00131231
31	47	D001451566
32	48	D006127170
33		D001451567
34	51	D001509536
35		D001509537
36		D001508609
37	52	D001501448
38		D001501575

39		D001501576
40		D001481096
41		D001481097
42	53	D001473219
43	55	D001452860
44		D001453776
45		D001456967
46		D001453796
47	56	D001453796
48	57	D001456730
49		D001453793
50	58	D001453825
51		D001453826
52		D001451047
53		D001451048
54		D001451049
55	59	D001453792
56	60	D001453857
57		D001453858
58		D001452875
59	61	D001451047
60		D001451048
61		D001451049
62		D001451050
63	62	D001280281
64		D001223783
65	63	D006127170
66	64	D000578523
67		D000327567
68		D000323071

69	66	FT 0000092
70		FT0002011
71	67	D003238683
72		D003238684
73		D003238662
74		D003238663
75		D003234997
76		D003234998
77		D003234999
78	69	D003230356
79		D003230357
80		D003230358
81	74	D002807543
82		D002744924
83	75	D002677551
84		D002677552
85	76	FT0002011
86	77	POS00158260
87		POS00158261
88		D002600066
89	80	D001834736
90		D001834737
91		D001829070
92		D001829141
93		D001823103
94	81	D001800067
95		D001798270
96	82	D001789135
97		D001789143
98		D010817600

99	83	D001789173
100		D001784134
101		D001774540
102	84	D001765641
103	86	D000523485
104		POS00399720
105	89	D000318982
106		D000318981
107	90	D000780551